

Splitting quaternion algebras over quadratic number fields*

Péter Kutas

Institute for Computer Science
and Control, Hungarian Acad.
Sci. and Department of Math-
ematics and its Applications,
Central European University
Kutas_Peter@phd.ceu.edu

June 6, 2016

Abstract

We propose an algorithm for finding zero divisors in quaternion algebras over quadratic number fields, or equivalently, solving homogeneous quadratic equations in three variables over $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer. The algorithm is deterministic and runs in polynomial time if one is allowed to call oracles for factoring integers and polynomials over finite fields.

Keywords: Explicit isomorphism, Full matrix algebra, Quadratic form, Quaternion algebra, Quadratic number field, Polynomial time algorithm.

Mathematics Subject Classification: 68W30, 16Z05, 11D09

1 Introduction

In this note we consider the following algorithmic problem which we call explicit isomorphism problem: let K be a field and let \mathcal{A} be a K -algebra isomorphic to $M_n(K)$ be given as a collection of structure constants (i.e. via its regular representation). The task is to construct an explicit isomorphism between \mathcal{A} and $M_n(K)$ or, equivalently, to find a primitive idempotent in \mathcal{A} .

Although the problem comes from computational representation theory, it has various applications in computational algebraic geometry and number theory as well. The case where $K = \mathbb{Q}$, has connections with explicit n -descent on elliptic curves [2], solving norm equations [7] and parametrizing Severi-Brauer surfaces [6]. The case where $K = \mathbb{F}_q$ is closely related to factorisation of polynomials over \mathbb{F}_p and the case where $K = \mathbb{F}_q(t)$ is connected to the factorisation problem in a certain skew-polynomial ring [4],[5] (this case is studied in [11]).

Ivanyos, Rónyai and Schicho proposed an ff-algorithm for the case where K is an algebraic number field [7]. An ff-algorithm is allowed to call oracles for factoring integers and polynomials

*An extended abstract containing part of the results was published in the conference proceedings MACIS 2015, LNCS 9582, pp. 1-6, 2016.

over finite fields. The cost of the call is the size of the input. Their algorithm however depends exponentially on the degree of the number field, the dimension of the matrix algebra and the logarithm of the discriminant of the number field. This algorithm was improved in [9].

In this note we consider the case where $\mathcal{A} \cong M_2(\mathbb{Q}(\sqrt{d}))$, where d is a square-free integer. Note that this problem is equivalent to solving homogeneous quadratic equations in 3 variables over quadratic number fields. We propose an ff-algorithm which solves the explicit isomorphism problem in polynomial time. This is an improvement on the results of [7] and [10], since those algorithms depend exponentially on $\log d$. The main idea of the algorithm is to find a subalgebra \mathcal{B} of \mathcal{A} which is a quaternion algebra over \mathbb{Q} . If \mathcal{B} is isomorphic to the full 2×2 matrix algebra over \mathbb{Q} then we use the algorithm from [7] (or [10]) to find a primitive idempotent. If not then we find an element $u \in \mathcal{B}$ such that $u^2 = d$ and return the zero divisor $u - \sqrt{d}$. From that one can construct an explicit isomorphism easily. Our main tools in solving these problems are the algorithms from Simon and Castel ([1],[14]) for finding zeros of quadratic forms in several variables.

The rest of the note is divided into two sections. In the first section we recall some basic facts and algorithms concerning quaternion algebras. In the second we describe our algorithm in detail.

2 Quaternion algebras

2.1 General properties

In this subsection we recall some basic facts about quaternion algebras. All these facts can be found in [15].

Definition 1. *Let K be a field. A central simple algebra \mathcal{A} over K is called a **quaternion algebra** if it has dimension 4 over K .*

A quaternion algebra has a special special K -basis as stated below:

Proposition 2. *Let $\text{char}(K) \neq 2$ and let H be a quaternion algebra over K . Then H has a K -basis $1, u, v, uv$ such that $uv = -vu$ and u^2 and v^2 are in the center of H . We call such a basis a quaternion basis of H .*

Remark 3. This result is well known, a proof can be found in [15]. There is a similar presentation if $\text{char}(K) = 2$, however since we will later only consider algebraic number fields, we omit this statement here.

From now on we assume that $\text{char}(K) \neq 2$. Since the center of H is K , we have that $u^2 \in K$ and $v^2 \in K$ if we identify 1 with the identity element of H . This motivates the following notation:

Definition 4. *Let H be a quaternion algebra over K with the quaternion basis $1, u, v, uv$. Let $u^2 = \alpha$ and $v^2 = \beta$. Note that α and β are in K . Then we denote H by $H_K(\alpha, \beta)$.*

It is easy to see that this is well-defined, i.e. all quaternion algebras which have a quaternion basis $1, u, v, uv$ such that $u^2 = \alpha$ and $v^2 = \beta$ are isomorphic.

The Wedderburn-Artin theorem implies that every quaternion algebra is either $M_2(K)$ or a division algebra over K . There is a nice criterion which tells us when a quaternion algebra is split (i.e., is isomorphic to $M_2(K)$). First we recall some definitions.

Definition 5. Let H be a quaternion algebra over K , with quaternion basis $1, u, v, uv$. Let $s = \lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv$. Then let $\sigma(s) = \lambda_1 - \lambda_2 u - \lambda_3 v - \lambda_4 uv$ be the **conjugate** of s . We call $\text{Tr}(s) = s + \sigma(s)$ the **trace** of s and $N(s) = s\sigma(s)$ the **norm** of s . Note that both $\text{Tr}(s)$ and $N(s)$ are in K .

Remark 6. One can show that the functions $\text{Tr}(x)$ and $N(x)$ do not depend on the quaternion basis and coincide with the usual reduced trace and reduced norm (see [15]).

Proposition 7. The following statements are equivalent:

1. $H_K(\alpha, \beta) \cong M_2(K)$,
2. There exists a nonzero element $s \in H_K(\alpha, \beta)$ such that $N(s) = 0$,
3. The quadratic form $x_1^2 - \alpha x_2^2 - \beta x_3^2 + \alpha\beta x_4^2$ is isotropic over K ,
4. There exists a nonzero element $s \in H_K(\alpha, \beta)$ such that $\text{Tr}(s) = 0$ and $N(s) = 0$,
5. The quadratic form $\alpha x^2 + \beta y^2 - z^2$ is isotropic over K .

If we write out condition (2) in terms of the quaternion basis we obtain (3). Condition (4) if written out would give the equation $\alpha x^2 + \beta y^2 - \alpha\beta z^2 = 0$ (since every traceless element is the linear combination of u, v and uv). By a change of variables we arrive at (5). Details can be found in [15] (or [1],[13]). Note that this shows that there is a strong connection between quaternion algebras and quadratic forms in three variables over K .

2.2 Algorithmic results

Now we review some algorithmic results concerning quaternion algebras and quadratic forms over \mathbb{Q} . In this section we consider an algebra to be given as a collection of structure constants, which means the following. Let \mathcal{A} be an algebra over the field K . Let a_1, \dots, a_m be a K -basis of \mathcal{A} . Then the products of the basis elements can be expressed as the K -linear combination of the basis elements:

$$a_i a_j = \gamma_{ij1} a_1 + \gamma_{ij2} a_2 + \dots + \gamma_{ijm} a_m.$$

The $\gamma_{ijk} \in K$ are called structure constants. Note that specifying \mathcal{A} with structure constants is equivalent to giving \mathcal{A} by its regular representation.

Example 8. Let $H_K(\alpha, \beta)$ be a quaternion algebra with the quaternion basis $1, u, v, uv$. Then every element is given by a 4×4 matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & \alpha & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \beta & 0 & 0 & 0 \\ 0 & -\beta & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -\alpha & 0 \\ 0 & \beta & 0 & 0 \\ -\alpha\beta & 0 & 0 & 0 \end{pmatrix}.$$

Rónyai [13] gave a polynomial time algorithm for finding a quaternion representation from an arbitrary structure constant representation. Thus we may assume that a quaternion algebra is given by a quaternion basis.

Definition 9. Let $\mathcal{A} \cong M_n(K)$ be given by structure constants. The **explicit isomorphism problem** is to compute an isomorphism between \mathcal{A} and $M_n(K)$.

Remark 10. Finding an explicit isomorphism is equivalent to finding an element r of rank 1 in \mathcal{A} . Indeed, the left action of A on the left ideal Ar produces such an isomorphism (the vector space Ar has dimension n and the left action is K -linear so every element of A can be represented by an $n \times n$ matrix and this map is an isomorphism).

Rónyai showed ([13]) that there is a randomized polynomial time reduction from the explicit isomorphism problem in the case $\mathcal{A} = M_2(\mathbb{Q})$ to factoring square-free integers. Ivanyos and Szántó [10] proposed a polynomial time ff-algorithm to solve this problem. They construct a maximal order (using the algorithm from [8]) and use lattice reduction to find a zero divisor. Cremona and Rusin gave a different algorithm [3] for the same task. They proposed an algorithm which solves homogeneous quadratic equations in three variables (these two tasks are equivalent). The algorithms from [6],[12] and [7] generalize these results to matrix algebras of higher degree.

However, if K is a number field then the algorithms from [7] and [10] run exponentially in the degree and the logarithm of the discriminant of the number field.

In the next section we consider the case where $\mathcal{A} \cong M_2(K)$ where K is a quadratic extension of \mathbb{Q} . It turns out that this is related to solving homogeneous quadratic equations in more than 3 variables. Hence we cite these two results:

Fact 1 (Simon [14]). *There is a polynomial time algorithm for solving homogenous quadratic equations over \mathbb{Q} in dimension 4 if one is allowed to call oracles for factoring integers.*

This task is also at least as hard as factoring integers since quadratic forms in dimension 4 with square discriminant correspond to quadratic forms of dimension 3 (see [1]). Simon also provided algorithms for higher dimension but they all use oracles for integer factorization. Castel [1] improved these algorithms and obtained an algorithm which works in dimension 5 (and above) and does not depend on factoring integers (it is, however, randomized).

Fact 2 (Castel [1]). *There is a randomized polynomial time algorithm which finds an isotropic vector for an indefinite quadratic form (over \mathbb{Q}) in dimension 5 (or more).*

3 Finding a zero divisor

In this section we propose an algorithm for finding a zero divisor in A which is isomorphic to $M_2(\mathbb{Q}(\sqrt{d}))$ and is given by structure constants. First we construct a subalgebra B in A which is a quaternion algebra over \mathbb{Q} . Then, with this information at our hands, we construct a zero divisor. In Remark 10 we saw how to construct an explicit isomorphism from a zero divisor. First we outline the steps of our algorithm:

Algorithm 1.

- Find an element $u \in \mathcal{A}$ such that $\text{Tr}(u) = 0$ and $u^2 \in \mathbb{Q}$ and $u \neq 0$.
- Find a nonzero element v such that $uv = -vu$ and $v^2 \in \mathbb{Q}$.
- Let B be the \mathbb{Q} -subspace generated by $1, u, v, uv$. B is a quaternion algebra over \mathbb{Q} . Use the algorithm from [7] (or [10]) to either find a zero divisor in B or conclude that B is a division algebra.
- If B is a division algebra then find an element $s \in B$ such that $s^2 = d$. Return $s - \sqrt{d}$.

The key to each step is finding an isotropic vector for a quadratic form in several variables. In Step 1 we solve a homogeneous quadratic equation in 6 variables, in Step 2 and 3 an equation in 3 variables and finally in Step 4 an equation in 4 variables. Now we proceed by providing an algorithm for each step.

Proposition 11. *Let $\mathcal{A} \cong M_2(\mathbb{Q}\sqrt{d})$ be given by structure constants. Then there exists a polynomial time ff-algorithm which finds a traceless nonzero $l \in \mathcal{A}$ (i.e. $\text{Tr}(l) = 0$), such that $l^2 \in \mathbb{Q}$.*

Proof. First we construct a quaternion basis $1, w, w', ww'$ of \mathcal{A} . We have the following:

$$w^2 = r_1 + t_1\sqrt{d}, \quad w'^2 = r_2 + t_2\sqrt{d}$$

If t_1 or t_2 is 0 then w or w' will be a suitable element. If $r_1t_2 + r_2t_1 = 0$ then $(ww')^2 \in \mathbb{Q}$ and is traceless. From now on we assume that t_1, t_2 and $r_1t_2 + r_2t_1$ are nonzero.

Every traceless element is in the $\mathbb{Q}(\sqrt{d})$ -subspace generated by w, w' and ww' . The condition $l^2 \in \mathbb{Q}$ gives the following equation ($s_1, \dots, s_6 \in \mathbb{Q}$):

$$((s_1 + s_2\sqrt{d})w + (s_3 + s_4\sqrt{d})w' + (s_5 + s_6\sqrt{d})ww')^2 \in \mathbb{Q}$$

If we expand this we obtain:

$$\begin{aligned} & ((s_1 + s_2\sqrt{d})w + (s_3 + s_4\sqrt{d})w' + (s_5 + s_6\sqrt{d})ww')^2 = \\ & (s_1^2 + ds_2^2 + 2s_1s_2\sqrt{d})(r_1 + t_1\sqrt{d}) + (s_3^2 + ds_4^2 + 2s_3s_4\sqrt{d})(r_2 + t_2\sqrt{d}) - \\ & (s_5^2 + ds_6^2 + 2s_5s_6\sqrt{d})(r_1 + t_1\sqrt{d})(r_2 + t_2\sqrt{d}) \end{aligned}$$

In order for this to be in \mathbb{Q} the coefficient of \sqrt{d} has to be zero:

$$\begin{aligned} & t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2 + t_2s_3^2 + t_2ds_4^2 + 2r_2s_3s_4 - (r_1t_2 + t_1r_2)s_5^2 - \\ & (r_1t_2 + t_1r_2)ds_6^2 - 2(r_1r_2 + t_1t_2d)s_5s_6 = 0 \end{aligned}$$

The left hand side of this equation is a quadratic form in 6 variables. This implies that if it is indefinite then it has a solution. First we calculate its Gram-matrix. It is block diagonal with three 2×2 blocks. The determinant of the first block is $t_1^2d - r_1^2$, the determinant of the second is $t_2^2d - r_2^2$ and the determinant of the third is $(r_1t_2 + t_1r_2)^2d - (r_1r_2 + t_1t_2d)^2$. Now we show that this quadratic form is always indefinite. If $d < 0$ then $t_1^2d - r_1^2 < 0$ (it is nonzero since $t_1 \neq 0$ and d is a square-free integer), hence the form $t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2$ is indefinite. If $d > 0$ then if either $t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2$ or $t_2s_3^2 + t_2ds_4^2 + 2r_2s_3s_4$ is indefinite then we are done. So the remaining case is when $t_1^2d - r_1^2 > 0$ and $t_2^2d - r_2^2 > 0$. However, this implies that the quadratic form $-(r_1t_2 + t_1r_2)s_5^2 - (r_1t_2 + t_1r_2)ds_6^2 - 2(r_1r_2 + t_1t_2d)s_5s_6$ is indefinite since

$$(t_1^2d - r_1^2)(t_2^2d - r_2^2) = -((r_1t_2 + t_1r_2)^2d - (r_1r_2 + t_1t_2d)^2)$$

Hence we have proven that the quadratic form

$$t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2 + t_2s_3^2 + t_2ds_4^2 + 2r_2s_3s_4 - (r_1t_2 + t_1r_2)s_5^2 - (r_1t_2 + t_1r_2)ds_6^2 - 2(r_1r_2 + t_1t_2d)s_5s_6 \quad (1)$$

is isotropic over \mathbb{Q} . An isotropic vector for the quadratic form in (1) can be found by Simon's algorithm [14]. This is an ff-algorithm which runs in polynomial time. \square

Remark 12. Observe that we only used the fact that \mathcal{A} is a quaternion algebra over $\mathbb{Q}(\sqrt{d})$, we did not need the fact that it is in fact a full matrix algebra.

Remark 13. The main tool of this proof was an algorithm for solving a homogeneous quadratic equation in 6 variables. For this task there is a randomized polynomial time algorithm described in [1]. Hence finding such an l can also be achieved in polynomial time. However, we would like our main algorithm to be deterministic so we cannot allow randomization here.

We proceed to the next step:

Proposition 14. *Let $\mathcal{B} = H_{\mathbb{Q}(\sqrt{d})}(a, b + c\sqrt{d})$ given by: $u^2 = a, v^2 = b + c\sqrt{d}$, where $a, b, c \in \mathbb{Q}$, $c \neq 0$. Then finding a nonzero element v' such that $uv' + v'u = 0$ and v'^2 is a rational multiple of the identity is equivalent to the explicit isomorphism problem for the quaternion algebra $H_{\mathbb{Q}}((\frac{b}{c})^2 - d, a)$.*

Proof. Since v' anticommutes with u (i.e. $uv' + v'u = 0$) it must be a $\mathbb{Q}(\sqrt{d})$ -linear combination of v and uv . This implies we have to search for $s_1, s_2, s_3, s_4 \in \mathbb{Q}$ such that:

$$((s_1 + s_2\sqrt{d})v + (s_3 + s_4\sqrt{d})uv)^2 \in \mathbb{Q}$$

Expanding this expression we obtain the following:

$$\begin{aligned} & ((s_1 + s_2\sqrt{d})v + (s_3 + s_4\sqrt{d})uv)^2 = \\ & (s_1^2 + s_2^2d + 2s_1s_2\sqrt{d})(b + c\sqrt{d}) - (s_3^2 + s_4^2d + 2s_3s_4\sqrt{d})a(b + c\sqrt{d}) \end{aligned}$$

In order for this to be rational, the coefficient of \sqrt{d} has to be zero. We obtain the following equation:

$$c(s_1^2 + s_2^2d) + 2bs_1s_2 - ac(s_3^2 + s_4^2d) - 2abs_3s_4 = 0$$

First we divide by c . Note that c is nonzero. Let $f = b/c$.

$$s_1^2 + s_2^2d + 2fs_1s_2 - a(s_3^2 + s_4^2d) - 2af s_3s_4 = 0 \tag{2}$$

In order to diagonalize the left hand side of (2), consider the following change of variables: $x := s_1 + fs_2$, $y := s_2$, $z := s_3 + s_4f$, $w := s_4$. Note that the transition matrix of this change is an upper triangular matrix with 1-s in the diagonal so it has determinant 1 (this means that these two equations are "equivalent"). In terms of these new variables the equation takes the following form:

$$x^2 + (d - f^2)y^2 - az^2 - a(d - f^2)w^2 = 0.$$

Finding a solution of this is equivalent to finding a zero divisor in the quaternion algebra $H_{\mathbb{Q}}(f^2 - d, a)$ by Proposition 7. \square

This statement can be interpreted both constructively and as a complexity statement as well. First it provides an ff-algorithm running in polynomial time for finding such an element v' . It also says however, that finding such an element v' is as hard as the explicit isomorphism problem for quaternion algebras. Rónyai proved in [13] that there is a randomized reduction from this task to factoring square-free integers. This implies that finding a quaternion subalgebra over \mathbb{Q} containing u is hard (otherwise one could easily find such an element v').

Finally putting Proposition 11 and 14 together we obtain the following:

Corollary 15. *Let $\mathcal{A} \cong M_2(\mathbb{Q}(\sqrt{d}))$ be given by structure constants. Then one can find a four dimensional subalgebra over \mathbb{Q} which is a quaternion algebra (and is split by $\mathbb{Q}(\sqrt{d})$) by an ff-algorithm which runs in polynomial time.*

Proof. First we find a traceless nonzero element l such that $l^2 \in \mathbb{Q}$ using the algorithm from Proposition 11. Now we prove that there exists an element l' such that $ll' + l'l = 0$ and $l'^2 \in \mathbb{Q}$.

There exists a subalgebra \mathcal{A}_0 in \mathcal{A} which is isomorphic to $M_2(\mathbb{Q})$. In this subalgebra there is an element l_0 for which l and l_0 have the same minimal polynomial over $\mathbb{Q}(\sqrt{d})$. This means that there exists an $m \in \mathcal{A}$ such that $l = m^{-1}l_0m$ ([15, Theorem 2.1.]). There exists a nonzero $l'_0 \in \mathcal{A}_0$ such that $l_0l'_0 + l'_0l_0 = 0$. Let $l' = m^{-1}l'_0m$. We have that $l'^2 = m^{-1}l'_0mm^{-1}l_0m = m^{-1}l_0^2m = l_0^2$, hence $l'^2 \in \mathbb{Q}$. Since conjugation by m is an automorphism we have that $ll' + l'l = m^{-1}(l_0l'_0 + l'_0l_0)m = m^{-1}0m = 0$. Thus we have proven the existence of a suitable element l' . Using the algorithm from Proposition 14 we can find an element l' such that $ll' + l'l = 0$ and $l'^2 \in \mathbb{Q}$.

The \mathbb{Q} -subspace generated by $1, l, l', ll'$ is a quaternion algebra H over \mathbb{Q} . Observe that $H \otimes \mathbb{Q}(\sqrt{d})$ has dimension 8 over \mathbb{Q} and is naturally embedded into $M_2(\mathbb{Q}(\sqrt{d}))$. Hence it must be $M_2(\mathbb{Q}(\sqrt{d}))$, so H is really split by $\mathbb{Q}(\sqrt{d})$. \square

An algorithm for the last two steps leads to our main theorem:

Theorem 16. *Let $\mathcal{A} \cong M_2(\mathbb{Q}(\sqrt{d}))$ be given by structure constants. Then there exists a polynomial time ff-algorithm which finds a zero divisor in \mathcal{A} .*

Proof. First we construct a quaternion subalgebra H over \mathbb{Q} using Corollary 15. If H is isomorphic to $M_2(\mathbb{Q})$, then one can find a zero divisor in it by using the algorithm from [7]. If not then there exists an element $s \in H$ such that $s^2 = d$. Indeed, since H is split by $\mathbb{Q}(\sqrt{d})$ and therefore contains $\mathbb{Q}(\sqrt{d})$ as a subfield [15, Theorem 1.2.8]. Let $1, u, v, uv$ be a quaternion basis with $u^2 = a, v^2 = b$. Every non-central element whose trace is zero (in H) is a \mathbb{Q} -linear combination of u, v and uv . Hence finding an element s such that $s^2 = d$ is equivalent to solving the following equation:

$$ax_1^2 + bx_2^2 - abx_3^2 = d \quad (3)$$

Since H is a division algebra, the quadratic form $ax_1^2 + bx_2^2 - abx_3^2$ is anisotropic. Thus solving equation (1) is equivalent to finding an isotropic vector for the quadratic form $ax_1^2 + bx_2^2 - abx_3^2 - dx_4^2$. One can find such a vector using the algorithm from [14]. This algorithm runs in polynomial time if one is allowed to call oracles for factoring integers. We have found an element s in H such that $s^2 = d$. Since H is a central simple algebra over \mathbb{Q} and d is not a square in \mathbb{Q} , the element s is not in the center of A . Hence $s - \sqrt{d}$ is a zero divisor in A . \square

Remark 17. An alternative ending of the algorithm could be the following. Assume that we have already found the subalgebra H . There always exists an element $s \in H$ for which $s^2 = d$. We have seen this in the case where H is a division algebra. If H is a matrix algebra then it is well-known. Hence the quadratic form $ax_1^2 + bx_2^2 - abx_3^2 - dx_4^2$ is always isotropic. We find an isotropic vector (x_1, x_2, x_3, x_4) . If $x_4 \neq 0$ we proceed as before. If $x_4 = 0$ then the norm of $x_1u + x_2v + x_3uv$ is 0, hence it is a zero divisor.

We conclude by stating that our algorithm can be used to solve quadratic equations in three variables over $\mathbb{Q}(\sqrt{d})$ by Proposition 7.

Acknowledgement The author would like to thank Gábor Ivanyos and Lajos Rónyai for their useful remarks and their constant support. Research supported by the Hungarian National Research, Development and Innovation Office - NKFIH.

References

- [1] P. Castel: Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation, Phd thesis, October 2011.
- [2] J.E. Cremona, T.A. Fisher, C. O’neill, D. Simon, M. Stoll: Explicit n -descent on elliptic curves III. Algorithms; Mathematics of Computation 84 No.292 (2015), 895-922.
- [3] J.E. Cremona, D. Rusin: Efficient solution of rational conics, Mathematics of Computation, 72 (2003), 1417-1441.
- [4] M. Giesbrecht, Y. Zhang: Factoring and decomposing Ore polynomials over $\mathbb{F}_q(T)$; Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation (ISSAC2003), New York, NY, USA: ACM. pp. 127-134.
- [5] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro: Factoring Ore polynomials over $\mathbb{F}_q(t)$ is difficult; (2015)Preprint arXiv:1505.07252.
- [6] W. A. de Graaf, M. Harrison, J. Pílnikova, J. Schicho: A Lie algebra method for rational parametrization of Severi-Brauer surfaces, Journal of Algebra, 303(2006), 514-529.
- [7] G. Ivanyos, L. Rónyai, J. Schicho: Splitting full matrix algebras over algebraic number fields, Journal of Algebra, 354(2012), 211-223.
- [8] G. Ivanyos, L. Rónyai: On the complexity of finding maximal orders in semisimple algebras over \mathbb{Q} ; Comput. complexity 3 (1993), pp. 245-261.
- [9] G. Ivanyos, Á. Lelkes, L. Rónyai: Improved algorithms for splitting full matrix algebras; JP Journal of Algebra, Number Theory and Applications 28 (2013), pp. 141-156.
- [10] G. Ivanyos, Á. Szántó: Lattice basis reduction for indefinite forms and an application, Discrete Mathematics 153 (1996), 177-188. MR 97c:11071
- [11] G. Ivanyos, P. Kutas, L. Rónyai: Computing explicit isomorphisms with full matrix algebras over $\mathbb{F}_q(x)$, (2015) Preprint arXiv: arXiv:1508.07755.
- [12] J. Pílniková: Trivializing a central simple algebra of degree 4 over the rational numbers, J. Symbolic Comput. 42(2007), 579-586.
- [13] L. Rónyai: Simple algebras are difficult; Proc. of the 19th Annual ACM Symposium on the Theory of Computing, New York (1987), 398-408.
- [14] D. Simon: Quadratic equations in dimensions 4, 5 and more, preprint (2005).
- [15] M-F. Vignéras: Arithmétique des Algèbres de Quaternions; Springer, LNM 800 (1980).